ONE IDENTITY™

One Identity Active Roles 7.2

Exchange Resource Forest Management Administrator Guide

Active Roles Exchange Resource Forest Management Administrator Guide
Updated - December 2017
Version - 7.2

Contents

Solution Overview

-
-
-

Understanding the problem

Although the majority of small- and medium-sized organizations deploy a single Active Directory forest, a significant portion of large organizations recognize and accommodate the need to deploy multiple forests. A multi-forest design carries higher administrative and support costs, and complicates collaboration and messaging. However, it offers the highest level of security isolation. In addition, some companies consider a multi-forest design because of organizational structure issues (such as autonomous business units and decentralized IT departments), business policy, or legal and regulatory requirements.

If a company chooses a multi-forest design, one of the main questions that arise is the setup of the Exchange messaging system.

An Exchange organization consists of one or more Exchange servers, and each Exchange organization is specific to one Active Directory forest. Exchange servers rely on access to the global catalog for address information. Because each forest has a separate global catalog, an Exchange organization is associated with only one forest.

Having multiple Exchange organizations hinders user collaboration and requires cross-forest replication of Exchange data between the organizations. To enable multiple Exchange organizations to function as a single business organization, additional configuration is required to synchronize the Exchange mail recipients in the respective directories in each Exchange organization.

Therefore, a preferred deployment option could be to have multiple forests use the same Exchange organization for mail service. A single Exchange organization that serves multiple forests does not require cross-forest synchronization of mail recipient data because the organization uses only one forest for its Active Directory storage and services.

Whether a single Exchange organization serves one forest or more than one forest, the Exchange organization is still associated with only one of the forests, called the *Exchange forest* (or resource forest). Users that have accounts in one forest might have mailboxes in

the same forest or in a different forest; however, mailboxes are always in the same forest as the Exchange servers because mailbox data is stored on the Exchange servers.

The following figure shows an Exchange organization that has mailboxes on Exchange servers in one forest and user accounts in a different forest. In this scenario, the user account in an accounts forest has a disabled account that represents the user's mailbox in the Exchange forest.

Figure 1: Processes automated by Active Roles SPML Provider
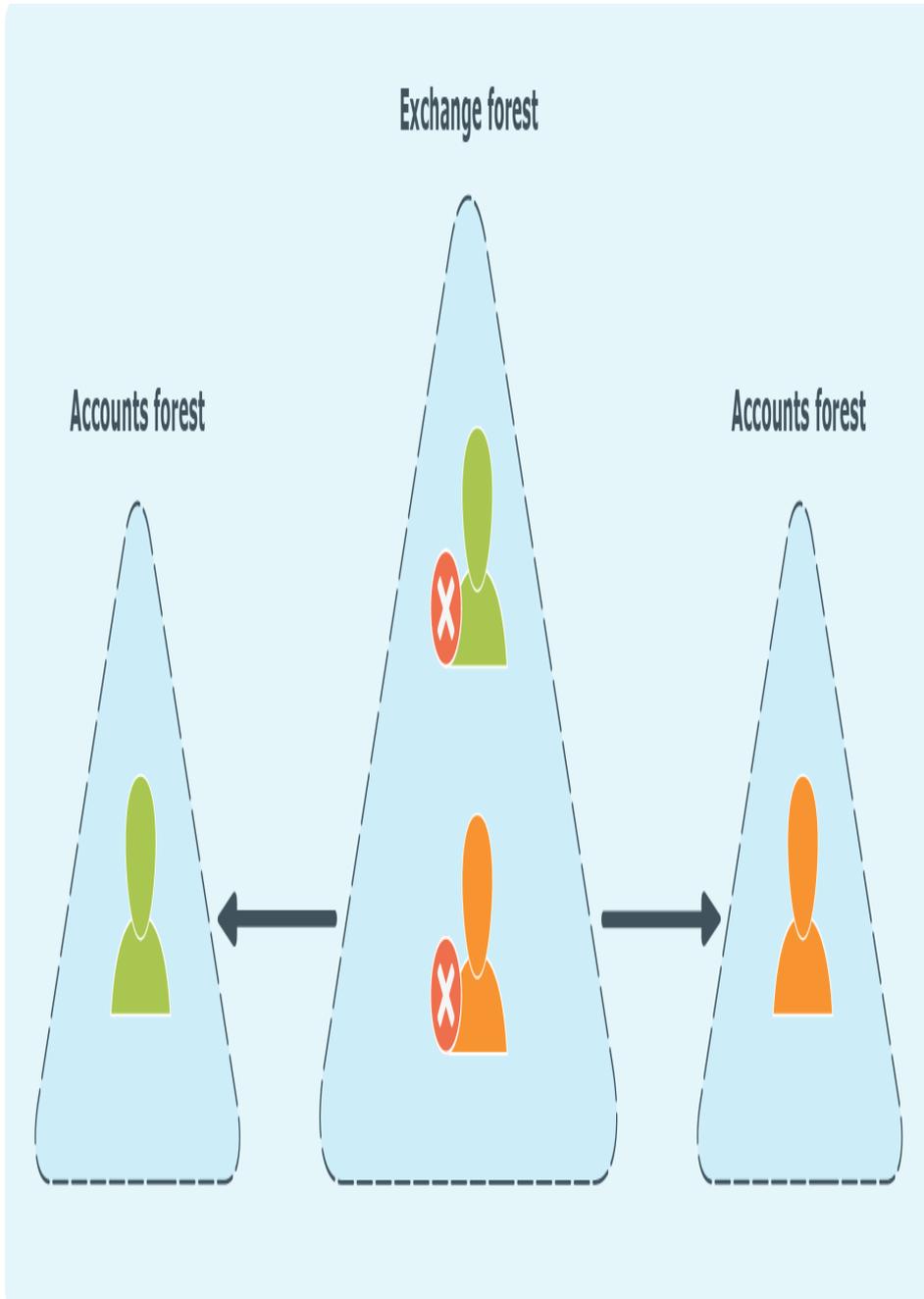
In the scenario where multiple forests share a single Exchange organization, Exchange servers are installed only in the Exchange forest. Users have their accounts in accounts forests and their mailboxes are stored in the Exchange forest. To associate a user with a mailbox, a disabled user account (shadow account) is created for that user in the Exchange forest. A mailbox is then created for the shadow account, with a certain attribute on the shadow account referencing the user's account held in the accounts forest. This type of Exchange environment is known as the *Exchange resource forest model*.

The main advantage of the Exchange resource forest model is a security boundary between Active Directory and Exchange administration. Also, a single Exchange organization provides for a single Global Address List (GAL), preserves all Exchange collaboration capabilities, and uses native Exchange data replication, thus lowering administrative overhead.

The major problem that arises in the resource forest model is that the separate Exchange forest and the various accounts forests require directory synchronization between them. A provisioning process needs to be set up so that each time an administrator creates a user account in an accounts forest, a shadow account with a mailbox is created in the Exchange forest. The account properties must also be synchronized between the accounts forest and the Exchange forest. These processes cannot be automated using native Active Directory mechanisms, which leads to the need for a third-party solution.

Understanding the solution

Exchange Resource Forest Management extends the Active Roles capabilities to enable the management of mailbox users in Exchange environments leveraging the resource forest model. The following figure illustrates the processes that are automated by Exchange Resource Forest Management.
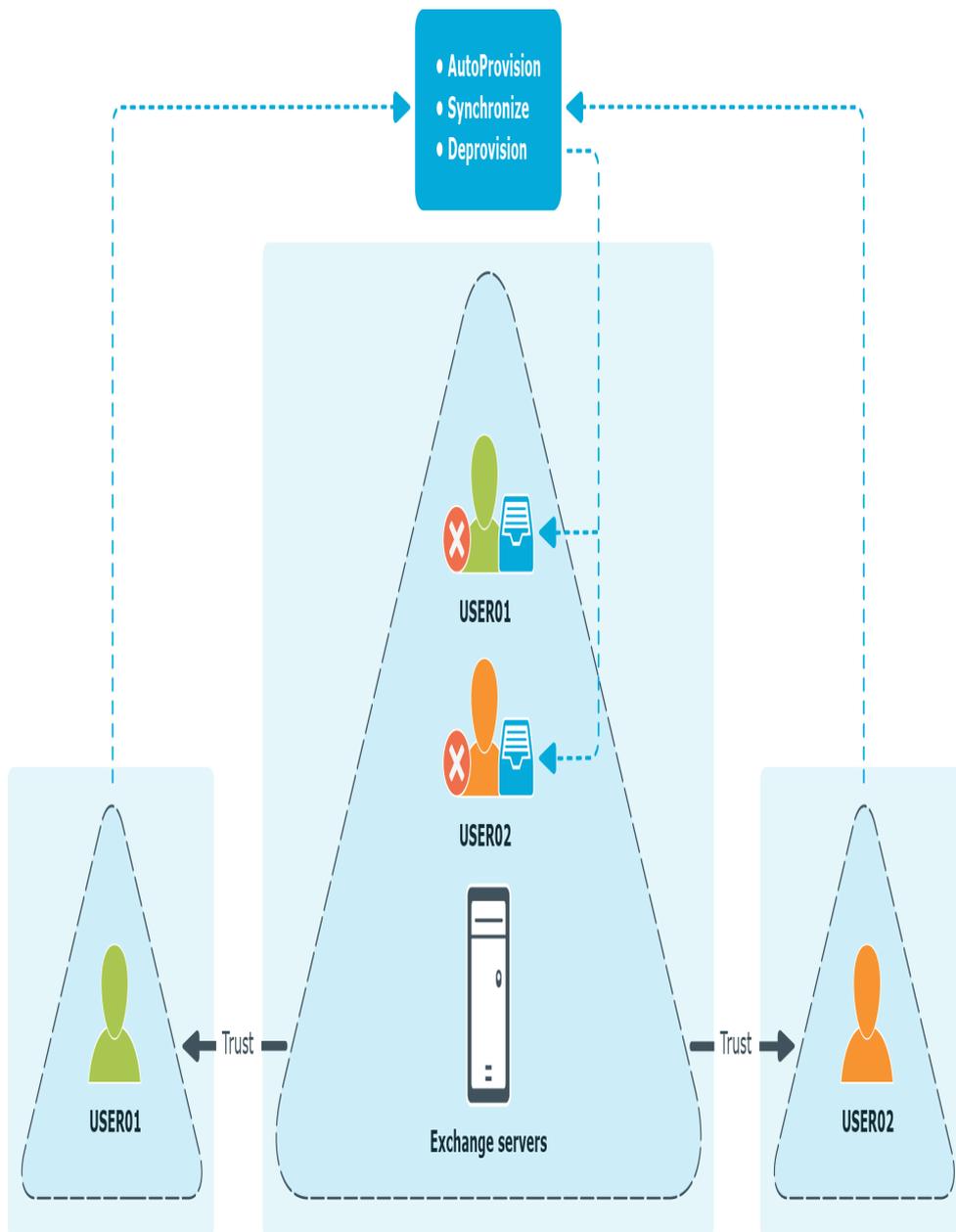
The AutoProvision, Synchronize, and Deprovision processes maintain the shadow accounts in the Exchange forest in sync with the master accounts upon creation, modification, deprovisioning, or deletion of master accounts in accounts forests.

AutoProvision

The AutoProvision process creates a shadow account in the Exchange forest upon:

- Creation of a user in the accounts forest if the option to create a mailbox for that user is selected
- Execution of the Exchange task to create a mailbox for an existing user from the accounts forest

Then, the AutoProvision process creates a linked mailbox associated with that shadow account, designating the user from the accounts forest as the linked master account for that mailbox.

To maintain a link between the master account and shadow account, Exchange Resource Forest Management assigns the globally unique identifier (GUID) of the shadow account to a certain attribute of the master account (the **adminDescription** attribute by default).

Normally, the AutoProvision process creates a shadow account with the same name as the name of the user from the accounts forest. In case of a name conflict, a different name is used to ensure the uniqueness of the shadow account's name.

Synchronize

The Synchronize process includes the following functions:

- Updating certain properties of shadow accounts based on changes to master accounts
- Substituting certain properties of master accounts with properties of shadow accounts
- Updating certain properties of master accounts based on changes to shadow accounts

Synchronized properties

When you update certain properties of a master account, Exchange Resource Forest Management updates those properties in both the master account and shadow account. These properties are referred to as *synchronized properties*.

Exchange Resource Forest Management performs synchronization of properties upon:

- Creation of shadow accounts
- Modification of master accounts

Thus, modifying personal or organization-related properties of a master account also results in updating those properties of the shadow account. This function ensures that changes to master accounts are properly reflected in the directory used by the Exchange messaging system. For the default list of synchronized properties, see Synchronized properties later in this document. You can configure Exchange Resource Forest Management to synchronize additional properties or remove individual properties from synchronization.

Substituted properties

When you view or change certain properties of a master account in an accounts forest, Exchange Resource Forest Management redirects the retrieval or change request to the properties of the shadow account in the Exchange forest. Such properties are referred to as *substituted properties*.

Thus, modification of Exchange-related properties of a master account only results in updating the corresponding properties of the shadow account. This function ensures that administration of master accounts properly manipulates Exchange recipient properties in the Exchange forest.

The substituted properties behave as follows:

- When retrieving property values for a master account, Active Roles returns the property values of the shadow account linked to the master account.

- When modifying properties for a master account, Active Roles actually updates the properties of the shadow account linked to the master account.

For the default list of substituted properties, see Substituted properties later in this document. You can configure Exchange Resource Forest Management to extend that list.

Back-synchronized properties

When you change certain properties of a shadow account, Exchange Resource Forest Management changes those properties in both the shadow account and master account. These properties are referred to as *back-synchronized properties*. By default, the list of back-synchronized properties consists of a single property—**mail (E-mail Address)**, and can be modified.

When a back-synchronized property of the shadow account has changed, Exchange Resource Forest Management replicates the change to the master account. The ability to replicate property changes from the shadow account to the master account is helpful in a situation where certain properties are administered on the shadow account rather than the master account.

Deprovision

The Deprovision process performs the deprovision operation on the shadow account once the master account is deprovisioned. This causes Active Roles to execute the deprovisioning policies that are in effect on the shadow account to deprovision the linked mailbox of the master account. Note that the mailbox deprovisioning policies must be applied to the container that holds shadow accounts rather than master accounts.

In Active Roles , you can undeprovision the deprovisioned master account. However, this may not undeprovision the shadow account (and, therefore, undeprovision the linked mailbox). For undeprovisioning master accounts to have an effect on shadow accounts, the

container that holds deprovisioned master accounts must be in the scope of the Policy Object provided by Exchange Resource Forest Management.

AutoProvision of distribution list manager

Exchange publishes distribution lists as mail-enabled groups in Active Directory. Such groups are listed in the Global Address List (GAL) and can be administered using Microsoft Outlook. Thus, Outlook can be used to add or remove members from a distribution list provided that the Outlook user is allowed to update the membership list of the respective group in Active Directory.

With Active Roles , an administrator can delegate the membership management task on a group to the account that is designated as the manager of the group. This can be done by specifying the manager's account on the **Managed By** page and then selecting the check box to allow the manager to update the membership list of the group. Both the group and the manager's account must be in the same Active Directory forest.

In the Exchange resource forest topology, where mail-enabled groups are located in the forest other than the forest containing user accounts, delegating the membership management task in this way is not feasible. To address the problem, Exchange Resource Forest Management synchronizes the manager setting for a shadow account on a group in the Exchange forest with the respective master account in the accounts forest, causing Active Roles to give the necessary rights to the master account.

If a user account (master account) in an accounts forest is configured to have a mailbox in the Exchange forest, and thus has a shadow account in the Exchange forest, the **Managed By** page can be used to give the master account the right to manage the membership list of a group. When you specify the shadow account as the manager of the group and select the check box to allow the manager to update the membership list, Exchange Resource Forest Management causes Active Roles to change security settings on the group so that the master account is authorized to add or remove members from the group.

Hence, on the **Managed By** page, you need to specify the shadow account rather than the master account. This requires a tool that would enable you to identify the shadow account. Exchange Resource Forest Management customizes the Active Roles Web Interface by adding a new entry to identify the shadow account. You can tell the shadow account's name and other properties from the **Shadow Account** tab on the **Exchange Properties** page for the master account.

Mailbox type conversion

You can use Active Roles to convert a linked mailbox to a user mailbox, and vice versa, by managing the mailbox in the Exchange forest.

For linked mailboxes in the Exchange forest, the Active Roles Web Interface provides a command allowing you to unlink the mailbox from the external user. The command converts the mailbox to the user mailbox type, and enables the user account associated

with the mailbox in the Exchange forest. The external user can no longer access the mailbox.

Foe user mailboxes in the Exchange forest, the Web Interface provides a command allowing you to link the mailbox to an external user from an accounts forest. The domain of the external user account must be registered with Active Roles (managed domain). The command converts the mailbox to the linked mailbox type, with the mailbox user in the Exchange forest configured as the shadow account and the external user specified as the linked master account.

For step-by-step instructions, see Mailbox type conversion later in this document.

Technical description

Exchange Resource Forest Management extends the mailbox management capabilities of Active Roles in the case of resource forest topology. This topology option assumes that you have:

- At least one Active Directory forest containing logon-enabled user accounts for your organization, referred to as an accounts forest. The accounts forest does not have Exchange Server installed, nor does it need to have the Active Directory schema extended with the Exchange Server attributes.

- An Active Directory forest with Exchange Server, referred to as the Exchange forest, to hold mailboxes for user accounts from the accounts forest.

- Trust relationships configured so that the Exchange forest trusts the accounts forest.

With Exchange Resource Forest Management, you can use Active Roles to:

- Create a mailbox for a user account from the accounts forest.

  You can create a mailbox when creating a user account in the accounts forest. It is also possible to create a mailbox for a user account that already exists in the accounts forest. As a result, Active Roles creates a disabled user account (shadow account) with a linked mailbox in the Exchange forest, and associates the shadow account and the mailbox with the user account (master account) held in the accounts forest.

- View or change mailbox properties, and perform Exchange tasks, on a user account from the accounts forest (master account) that has a linked mailbox in the Exchange forest.

  The pages for managing the master account include all Exchange properties and tasks that are normally available when the mailbox resides in the same forest as the managed user account. With Exchange Resource Forest Management, Active Roles synchronizes the Exchange properties displayed or changed on the pages for managing the master account with the properties of the linked mailbox.

- View or change the personal or organization-related properties of the master account while having them synchronized to the respective properties of the shadow account.

  When you use Active Roles to change the personal or organization-related properties

of the master account, Exchange Resource Forest Management causes Active Roles to apply the changes to those properties of the shadow account as well. This function ensures correct information about the master account in the Exchange address lists.

- Deprovision a master account while having Active Roles deprovision the master account's mailbox in the Exchange forest.

  When you deprovision a master account, Exchange Resource Forest Management causes Active Roles to apply the deprovisioning policies to both the master account and shadow account. As a result, Active Roles makes all the necessary changes to deprovision the mailbox. You can revert these changes by undeprovisioning the master account.

- Delegate Exchange mailbox management tasks by applying Access Templates to containers that hold master accounts.

  For example, you can apply the "Exchange - Recipients Full Control" Access Template to a container in the accounts forest, which enables the delegated administrator to create, view or change linked mailboxes in the Exchange forest by managing master accounts held in that container.

- Enable a master account to update membership list of a distribution group held in the Exchange forest.

  When you make a shadow account the manager or a secondary owner of a distribution group and allow the manager or secondary owners to update membership list, Exchange Resource Forest Management ensures that the corresponding master account has sufficient rights to add or remove members from that group using Exchange clients such as Microsoft Outlook or Outlook Web App.

Exchange Resource Forest Management also enables Active Roles to provide all these administrative capabilities for linked mailboxes created by Active Roles with an earlier version of Exchange Resource Forest Management or without Exchange Resource Forest Management, or created by tools other than Active Roles . Exchange Resource Forest Management schedules Active Roles to search the managed domains for linked mailboxes whose master account:

- Is in the scope of the Exchange Resource Forest Management policy for mailbox management
- Does not have a reference to the shadow account expected by Exchange Resource Forest Management

For each master account that meets these conditions, Active Roles updates the master account with a reference to the shadow account, thereby extending the capabilities of Exchange Resource Forest Management to that master account and its linked mailbox. As a result, the linked mailbox falls under the control of Exchange Resource Forest Management.

Policy Object

Exchange Resource Forest Management uses a Policy Object to implement mailbox management policy for Exchange resource forest topology. This policy enables Active Roles to create and manage linked mailboxes in the resource forest by administering linked master accounts in an accounts forest. The Policy Object is in the **Configuration/Policies/Administration/Builtin** container. The name of the Policy Object is **Built-in Policy - ERFM - Mailbox Management**.

To enable Exchange Resource Forest Management, you need to apply that Policy Object to the domain or container that holds linked master accounts you want Active Roles to administer.

Policy settings

The topics in this section cover the mailbox management policy settings.

Container for new shadow accounts

The policy allows you to specify the container in which you want Active Roles to create shadow accounts when creating linked mailboxes managed by Exchange Resource Forest Management. You can select the desired organizational unit in the Exchange forest or you can let Active Roles choose the default container.

If you select a particular organizational unit, Active Roles creates shadow accounts in that organizational unit. You can select an organizational unit from any domain of the Exchange forest that is registered with Active Roles as a managed domain.

If you let Active Roles choose the default container for new shadow accounts, then Active Roles creates shadow accounts in the **Users** container in a particular domain of the Exchange forest. If the forest root domain of the Exchange forest is registered with Active Roles as a managed domain, then Active Roles creates shadow accounts in that domain. Otherwise, Active Roles creates shadow accounts in the domain that appears first in the ordered list of the managed domains from the Exchange forest. Note that Exchange Resource Forest Management requires at least one domain of the Exchange forest to be registered with Active Roles as a managed domain.

Default description for new shadow accounts

The policy allows you to specify a text to use as the default description for new shadow accounts that Active Roles creates when creating linked mailboxes managed by Exchange Resource Forest Management. Active Roles writes that text to the **Description** property of every new shadow account.

Attribute to store a reference to shadow account

By default, the policy designates the **adminDescription** attribute of the master account for storing the GUID of the shadow account, and allows you to choose a different attribute for that purpose. Exchange Resource Forest Management uses this attribute to identify the shadow account (and, consequently, the linked mailbox) when managing a given master account. The policy causes Active Roles to set this attribute on the master account when creating the linked mailbox.

Synchronized properties

The policy defines a list of properties to copy from the master account to the shadow account. These properties are referred to as *synchronized properties*. When you use Active Roles to set or change a synchronized property of a master account, the policy causes Active Roles to set or change the value of that property on both the master account and shadow account.

In addition, Exchange Resource Forest Management provides a scheduled task that copies synchronized properties from every managed master account to the corresponding shadow account. The task runs on a scheduled basis to ensure that each of the synchronized properties of the shadow account has the same value as the corresponding property of the master account. If a synchronized property of the shadow account has changed for whatever reason, Active Roles changes that property back to the value found on the master account. For further details, see Scheduled Task later in this document.

The following table provides the default list of synchronized properties. You can configure the policy to synchronize additional properties or remove individual properties from synchronization.

Table 1: Default list of synchronized proprties

c (Country Abbreviation)	physicalDeliveryOfficeName (Office Location)
co (Country)	postalCode (ZIP/Postal Code)
company (Company)	postOfficeBox (Post Office Box)
countryCode (Country-Code)	sAMAccountName (Logon Name (pre-Windows 2000))
department (Department)	
displayName (Display Name)	sn (Last Name)
givenName (First Name)	st (State/Province)
homePhone (Home Phone)	streetAddress (Street Address)
initials (Initials)	telephoneNumber (Telephone Number)
l (City)	title (Job Title)
mobile (Mobile Number)	url (Web Page Address (Others))
otherTelephone (Phone Number (Others))	

Substituted properties

The policy defines a list of properties that appear on the master account but reflect the properties of the linked mailbox or shadow account. These properties are referred to as *substituted properties*. When you use Active Roles to view properties of a master account, the policy causes Active Roles to retrieve the values of the master account's substituted properties from the shadow account. When you use Active Roles to set or change a substituted property of a master account, the policy causes Active Roles to set or change the value of that property on the shadow account.

The policy adds all the Exchange recipient properties to the default list of substituted properties, which causes Active Roles to operate as if master accounts have those properties although the accounts forest does not have Exchange Server installed (and, therefore, does not have the Active Directory schema extended with Exchange recipient properties).

The policy does not allow you to narrow down the list of substituted properties. However, you can specify your custom list of substituted properties in addition to the default list. If you do so, the resulting list of substituted properties includes all properties from both the default list and your custom list.

Table 2: Default list of substituted properties

adminDisplayName	edsva-MsExch-AllowRecurringMeetings
altRecipient	edsva-MsExch-AllRequestInPolicy
altRecipientBL	edsva-MsExch-AllRequestOutOfPolicy
authOrig	edsva-MsExch-ApplyEmailAddressPolicy
authOrigBL	edsva-MsExch-ArchiveMailboxDatabase
autoReply	edsva-MsExch-ArchiveMailboxEnabled
autoReplyMessage	edsva-MsExch-ArchiveMailboxName
deletedItemFlags	edsva-MsExch-ArchiveMailboxQuota
delivContLength	edsva-MsExch-ArchiveMailboxWarningQuota
deliverAndRedirect	
deliveryMechanism	edsva-MsExch-AutoReplyExternalAudience
delivExtContTypes	edsva-MsExch-AutoReplyExternalMessage
displayNamePrintable	edsva-MsExch-AutoReplyInternalMessage
dLMemDefault	edsva-MsExch-AutoReplyState
dLMemRejectPerms	edsva-MsExch-BookingWindowInDays
	edsva-MsExch-BookInPolicy-DN

dLMemSubmitPerms

dnQualifier

edsaAdminGroup

edsaAllExchangeTasks

edsaCreateMsExchMailbox

edsaDeleteEmail

edsaDeleteMailbox

edsaEstablishEmail

edsaEstablishGroupEmail

edsaExchangeTasksAvailable

edsaHideMembership

edsaHomeMDB

edsaHomeMTA

edsaMailboxSecurityDescriptor

edsaMoveMailbox

edsaMsExchMixedMode

edsaRemoveAllMsExchAttributes

edsaUnhideMembership

edsvaExchOrgVersion

edsvaExchServerVersion

edsva-MsExch-AcceptMessagesOnlyFrom

edsva-MsExch-ActiveMailboxServerName

edsva-MsExch-AddAdditionalResponse

edsva-MsExch-AdditionalResponse

edsva-MsExch-AddNewRequestsTentatively

edsva-MsExch-AddOrganizerToSubject

edsva-MsExch-AddressBookPolicyDN

edsva-MsExch-AllBookInPolicy

edsva-MsExch-AllowConflicts

edsva-MsExch-ProtocolSettings-IMAP4-Enable

edsva-MsExch-ProtocolSettings-MAPI-Enable

edsva-MsExch-ProtocolSettings-OMA-Enable

edsva-MsExch-BypassModerationFor

edsva-MsExch-ConflictPercentageAllowed

edsva-MsExch-DeleteAttachments

edsva-MsExch-DeleteComments

edsva-MsExch-DeleteNonCalendarItems

edsva-MsExch-DeleteSubject

edsva-MsExch-EnableArchiveMailbox

edsva-MsExch-EnableCalendarAttendant

edsva-MsExch-EnableResourceBookingAttendant

edsva-MsExch-EndDateForRetentionHold

edsva-MsExch-EnforceSchedulingHorizon

edsva-MsExch-ForwardRequestsToDelegates

edsva-MsExch-LitigationHoldEnabled

edsva-MsExch-MailboxItemsTotal

edsva-MsExch-MailboxLastLoggedOnBy

edsva-MsExch-MailboxSize

edsva-MsExch-MaximumConflictInstances

edsva-MsExch-MaximumDurationInMinutes

edsva-MsExch-MemberDepartRestriction

edsva-MsExch-MemberJoinRestriction

edsva-MsExch-ModeratedBy

edsva-MsExch-ModerationEnabled

edsva-MsExch-ModerationNotificationSending

edsva-MsExch-MoveRequestStatus

edsva-MsExch-OrganizerInfo

edsva-MsExch-ProcessExternalMeetingMessages

edsva-MsExch-ProtocolSettings-ActiveSync-Enable

edsva-MsExch-ProtocolSettings-ActiveSync-PolicyDN

edsva-MsExch-ProtocolSettings-IMAP4-Config

ONE IDENTITY™

edsva-MsExch-ProtocolSettings-OWA-Enable

edsva-MsExch-ProtocolSettings-POP3-Config

edsva-MsExch-ProtocolSettings-POP3-Enable

edsva-MsExch-ProtocolSettings-UpToDateNotifications-Enable

edsva-MsExch-RejectMessagesFrom

edsva-MsExch-RemoveForwardedMeetingNotifications

edsva-MsExch-RemoveMoveRequest

edsva-MsExch-RemoveOldMeetingMessages

edsva-MsExch-RemovePrivateProperty

edsva-MsExch-RequestInPolicy-DN

edsva-MsExch-RequestOutOfPolicy-DN

edsva-MsExch-RequireSenderAuthentication

edsva-MsExch-ResourceCapacity

edsva-MsExch-ResourceCapacity

edsva-MsExch-ResourceCustomProperties

edsva-MsExch-ResourceDelegates-DN

edsva-MsExch-RetentionComment

edsva-MsExch-RetentionHoldEnabled

edsva-MsExch-RetentionPolicy-DN

edsva-MsExch-RetentionUrl

edsva-MsExch-RoleAssignmentPolicyDN

edsva-MsExch-ScheduleOnlyDuringWorkHours

edsva-MsExch-SharedMailboxUsers

edsva-MsExch-SharingPolicyDN

edsva-MsExch-StartDateForRetentionHold

edsva-MsExch-TentativePendingApproval

edsva-MsExch-UMAnonymousCallersCanLeaveMessages

enabledProtocols

expirationTime

extensionAttribute1

extensionAttribute13

extensionAttribute14

extensionAttribute15

extensionAttribute2

extensionAttribute3

extensionAttribute4

extensionAttribute5

extensionAttribute6

extensionAttribute7

extensionAttribute8

extensionAttribute9

extensionData

folderPathname

formData

forwardingAddress

garbageCollPeriod

heuristics

homeMDB

homeMTA

importedFrom

internetEncoding

language

languageCode

legacyExchangeDN

mail

mailNickname

mAPIRecipient

mDBOverHardQuotaLimit

mDBOverQuotaLimit

mDBStorageQuota

mDBUseDefaults

ONE IDENTITY™

edsva-MsExch-UMAutomaticSpeechRecognitionEnabled

edsva-MsExch-UM-CallAnsweringRulesEnabled

edsva-MsExch-UM-CallsFromNonUsersAllowed

edsva-MsExch-UM-DialPlanDN

edsva-MsExch-UM-ExtensionNumbers

edsva-MsExch-UM-FaxEnabled

edsva-MsExch-UM-IsEnabled

edsva-MsExch-UM-LockedOut

edsva-MsExch-UM-MailboxPolicyDN

edsva-MsExch-UM-OperatorExtensionNumber

edsva-MsExch-UM-PIN

edsva-MsExch-UM-PINResetOnFirstLogon

edsva-MsExch-UM-SIPAddress

edsvaSendAsTrustees

msExchHideFromAddressLists

msExchHomeServerName

msExchIMACL

msExchIMAddress

msExchIMAPOWAURLPrefixOverride

msExchIMMetaPhysicalURL

msExchIMPhysicalURL

msExchIMVirtualServer

msExchInconsistentState

msExchMailboxFolderSet

msExchMailboxGuid

msExchMailboxSecurityDescript
or
msExchMailboxUrl

msExchMasterAccountSid

msExchMobileMailboxPolicyLink

msExchOmaAdminExtendedSettings

msExchADCGlobalNames

msExchALObjectVersion

msExchConferenceMailboxBL

msExchControllingZone

msExchCustomProxyAddresses

msExchExpansionServerName

msExchFBURL

msExchTUIPassword

msExchTUISpeed

msExchTUIVolume

msExchUnmergedAttsPt

msExchUseOAB

msExchUserAccountControl

msExchVoiceMailboxID

oOFReplyToOriginator

pOPCharacterSet

pOPContentFormat

preferredDeliveryMethod

protocolSettings

proxyAddresses

publicDelegates

publicDelegatesBL

queryPolicyBL

replicatedObjectVersion

replicationSensitivity

replicationSignature

reportToOriginator

reportToOwner

securityProtocol

serverReferenceBL

showInAddressBook

submissionContLength

targetAddress

textEncodedORAddress

msExchOmaAdminWirelessEnable   unauthOrig

msExchOriginatingForest   unmergedAtts

msExchPfRootUrl

msExchPoliciesExcluded

msExchPoliciesIncluded

msExchPolicyEnabled

msExchPolicyOptionList

msExchPreviousAccountSid

msExchProxyCustomProxy

msExchQueryBaseDN

msExchRecipLimit

msExchRequireAuthToSendTo

msExchResourceGUID

msExchResourceProperties

Back-synchronized properties

The policy defines a list of properties to copy from the shadow account to the master account. By default, the list contains a single property, **E-Mail Address (mail)**. When the e-mail address has changed on the shadow account (which is normally the case when Exchange Server creates a linked mailbox), the policy ensures that the e-mail address is correctly set on the master account by copying the e-mail address form the shadow account.

Policy actions

The mailbox management policy causes Active Roles to perform the following actions depending on the change request submitted to the Active Roles Administration Service.

Table 3: Policy actions

Request	Actions
Create a new user with mailbox	Active Roles creates the new user (in the accounts forest), and then performs the following actions:
	• Create a shadow account (in the Exchange forest), and populate its properties with the data found in the request
	• Create a linked mailbox using that shadow account, with

Request	Actions
	the new user (from the accounts forest) specified as the linked master account
	• Create a reference to the shadow account on the master account
	• Update the master account with the e-mail address of the linked mailbox
	When creating the shadow account or mailbox, Active Roles executes all policies that are applied to the container that holds the shadow account, including the mailbox auto-provisioning policies (if any). To have an effect, mailbox auto-provisioning policies must be applied to the container that holds shadow accounts (rather than master accounts).
Create a mailbox for an existing user	Active Roles retrieves the properties of the existing user (in the accounts forest), and then performs the following actions:
	• Create a shadow account (in the Exchange forest), and populate its properties with the properties of the existing user
	• Create a linked mailbox using that shadow account, with the existing user (from the accounts forest) specified as the linked master account
	• Create a reference to the shadow account on the master account
	• Update the master account with the e-mail address of the linked mailbox
	When creating the shadow account or mailbox, Active Roles executes all policies that are applied to the container that holds the shadow account, including the mailbox auto-provisioning policies (if any). To have an effect, mailbox auto-provisioning policies must be applied to the container that holds shadow accounts (rather than master accounts).
Modify properties of a master account	If the change request includes any changes to substituted properties, Active Roles he requested changes to the substituted properties of the shadow account. Next, Active Roles makes the requested changes to the properties of the master account, and then updates the synchronized properties of the shadow account with the new property values found on the master account.
Perform an Exchange task on a master account	Active Roles applies the Exchange task to the shadow account of that master account.

Request	Actions
Deprovision a master account	Active Roles deprovisions the master account, and then deprovisions the shadow account. When deprovisioning the shadow account, Active Roles executes all deprovisioning policies that are applied to the container that holds the shadow account, including the mailbox deprovisioning policies. To have an effect, mailbox deprovisioning policies must be applied to the container that holds shadow accounts (rather than master accounts).
Undeprovision a deprovisioned master account	Active Roles undeprovisions the master account and then undeprovisions the shadow account. Once the shadow account has been undeprovisioned, the master account's mailbox reverts to the state it was in before the master account was deprovisioned. For undeprovisioning master accounts to have an effect on shadow accounts, the container that holds deprovisioned master accounts must be in the scope of the **Built-in Policy - ERFM - Mailbox Management** Policy Object (or a copy of that Policy Object).
Delete a master account	Active Roles deletes the master account, and then performs the "Disable mailbox" task on the shadow account.

Scheduled Task

Exchange Resource Forest Management includes an Active Roles scheduled task that complements the mailbox management policy to enforce synchronization of master and shadow account properties, and to capture existing linked mailboxes whose master account is put under the control of that policy. The scheduled task object is in the **Configuration/Server Configuration/Scheduled Tasks/Builtin** container. The name of the object is **ERFM - Mailbox Management**. The task is scheduled to run on a daily basis. Normally, you do not need to modify that scheduled task.

The operation of the task affects only the user accounts that are in the scope of the **Built-in Policy - ERFM - Mailbox Management** Policy Object (or a copy of that Policy Object). When run, the task performs the following actions on each of those user accounts:

- If the user account does not have a linked mailbox, then skip over that user account.

- If the user account has a linked mailbox but does not store a reference to the shadow account of that mailbox, then create the reference to the shadow account on that user account.

  This action enables Exchange Resource Forest Management to administer exiting linked mailboxes, possibly created using an earlier version of Exchange Resource Forest Management or without the use of Exchange Resource Forest Management.

- If the user account has a linked mailbox and stores a reference to the shadow account, then copy the synchronized properties from the master account to the shadow account, and copy the back-synchronized properties from the shadow account to the master account.

  This action ensures that the shadow account properties are updated with the latest changes to the master account properties and vice versa.

- If the shadow account is the manager (or a secondary owner) who can update membership list of a particular group, then the task checks that group to see if the master account can update membership list as well, and, if necessary, gives the master account the right to update membership list.

  This action synchronizes the group manager rights of the master account with the group manager rights of the shadow account, thereby enabling the mailbox logon account (which is the master account) to add or remove members from distribution lists by using Outlook or Outlook Web App.

Deploying the Solution

- Prerequisite conditions
- Applying the Policy Object
- Upgrade from an earlier version

Prerequisite conditions

This section summarizes the prerequisite conditions that must be met before you deploy Exchange Resource Forest Management.

Exchange Server deployment

Exchange Resource Forest Management requires Exchange 2010 or later to be deployed in the Exchange forest.

Exchange Server should not be installed in the accounts forests. The Active Directory schema in the accounts forests does not need to be extended with the Exchange Server attributes.

A trust between the Exchange forest and the accounts forest must be set up before you can use Exchange Resource Forest Management. At a minimum, an outgoing trust must be set up so that the Exchange forest trusts the accounts forest.

For more information, see "Learn more about setting up a forest trust to support linked mailboxes" at http://technet.microsoft.com/library/ms.exch.eac.trustedforestordomainlearnmore (v=exchg.150).aspx.

Active Roles deployment

The following Active Roles components must be installed in your Active Directory environment:

- Administration Service
- Web Interface
- Active Roles console

You can install these components on member servers in an accounts forest or in the Exchange forest. For installation instructions, see the Active Roles Quick Start Guide.

Log on as Active Roles Admin

To configure Exchange Resource Forest Management, log on as Active Roles Admin. This ensures that you have sufficient rights to make the necessary configuration changes. Assuming the default configuration of the Active Roles Administration Service, you should log on with a domain user account that is a member of the Administrators group on the computer running the Administration Service.

Register domains with Active Roles

Exchange Resource Forest Management requires the following domains to be registered with Active Roles :

- In the Exchange forest, a domain that hold computers running the Mailbox server role
- In each accounts forest, the domains that hold the users you want to administer with Active Roles

When registering a domain, you are prompted to choose which account you want the Administration Service to use to access the domain. You can either specify a so-called *override account* or let the Administration Service use its service account. With either option, the account must have sufficient rights in the domain you are registering. At a minimum, the account must have the following rights:

- Member of the **Account Operators** domain security group
- In case of Exchange 2010 or 2013, member of the **Recipient Management** role group in the Exchange forest (see "Access to Exchange Server/Exchange 2010" or "Access to Exchange Server/Exchange 2013" in the Active Roles Quick Start Guide), and enabled for remote Exchange Management Shell (see "Support for remote Exchange Management Shell" in the Active Roles Quick Start Guide)
- In the Exchange forest, read access to Exchange configuration data (see "Permission to read Exchange configuration data" in the Active Roles Quick Start Guide).

For instructions on how to register domains with Active Roles , see "Adding and removing managed domains" in the Active Roles Administrator Guide.

Applying the Policy Object

Active Roles provides a built-in Policy Object containing the mailbox management policy for Exchange resource forest topology. To enable Exchange Resource Forest Management, you need to:

Link that Policy Object to the appropriate containers in the accounts forest. These are the containers that hold the user accounts you want to administer using Exchange Resource Forest Management.

Optionally, view or change policy settings.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.

2. In the details pane, right-click the **Built-in Policy - ERFM - Mailbox Management** Policy Object, and then click **Policy Scope**.

3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain in the accounts forest.

Out of the box, the Policy Object has all policy settings configured. You can use the Active Roles console to view or change policy settings as needed.

To view or change policy settings

1. Double-click the **Built-in Policy - ERFM - Mailbox Management** Policy Object.

2. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.

3. In the **Properties** dialog box that appears, do any of the following:

   a. On the **Shadow Account** tab, view or change the container and default description for new shadow accounts.

   b. On the **Master Account** tab, view or change the attribute to store a reference to shadow account.

   c. On the **Synced** tab, view or change the list of synchronized properties.

   d. On the **Substituted** tab, configure your custom list of substituted properties in addition to the default list.

   e. On the **Back-synced** tab, view or change the list of back-synchronized properties.

For detailed description of the policy settings, see Policy settings earlier in this document.

Upgrade from an earlier version

You can seamlessly upgrade from Quick Connect for Exchange Resource Forests to Exchange Resource Forest Management, as follows.

1. Inspect your current configuration of Quick Connect for Exchange Resource Forests, and note down the existing policy settings such as:

   - The container for new shadow accounts, identified by the **Default Mailbox OU** policy parameter.

   - The default description for new shadow accounts, identified by the **Shadow account description** policy parameter.

   - The attribute to store a reference to shadow account, identified by the **Attribute to store back link** policy parameter.

   - The list of synchronized properties, identified by the **Synchronized Attributes List** policy parameter.

   - The custom list of substituted properties (if any)), identified by the **Substituted Attributes List** policy parameter.

   - The list of back-synchronized properties, identified by the **Back-synchronized attributes list** policy parameter.

   For instructions on how to access policy parameters, see the "Set Up and Apply the Policy Objects" topic in the Quick Connect for Exchange Resource Forests Administrator Guide.

2. Uninstall the earlier version of the ERFM add-on from the system.

> ⓘ NOTE: If ERFM (Exchange Resource Forest Management) is installed on the Active Roles 6.x version, it must be uninstalled before installing Active Roles 7.1, as ERFM is now part of the product. Failure to uninstall ERFM may result in conflicts and issuese-place this text with a description of a feature that is noteworthy.

3. Upgrade to Active Roles version 7.2. For upgrade instructions, see the Active Roles 7.2 Quick Start Guide.

4. Adjust the policy settings in the Exchange Resource Forest Management Policy Object to match the settings you noted down in Step 1, and then link that Policy Object to the containers that hold the master accounts you managed using Quick Connect for Exchange Resource Forests. For instructions on how to configure and link that Policy Object, see Applying the Policy Object earlier in this document.

After you have performed these steps, Exchange Resource Forest Management recognizes the existing master accounts, enabling Active Roles to manage their linked mailboxes in the same way as when using Quick Connect for Exchange Resource Forests.

To expedite the recognition of the existing master accounts, you might execute the Exchange Resource Forest Management scheduled task without waiting for its scheduled run: In the Active Roles console, navigate to the **Configuration/Server Configuration/Scheduled Tasks/Builtin** container, right-click the task **ERFM - Mailbox Management** in that container, point to **All Tasks**, and then click **Execute**.

Examples of Use

- Configuration
- Mailbox creation
- Account modification
- Account deprovisioning
- Membership management delegation
- Mailbox type conversion

Configuration

The examples in this chapter assume the following configuration of Exchange Resource Forest Management:

- **Accounts** is the name of an organizational unit in a managed domain of an accounts forest.
- **Mailboxes** is the name of an organizational unit in a managed domain of the Exchange forest.
- The the **Built-in Policy - ERFM - Mailbox Management** Policy Object is linked to the **Accounts** OU.
- In the policy settings, the **Mailboxes** OU is selected as the container for new shadow accounts. Other policy settings are not modified so they have the default values.

In other words, the **Accounts** OU holds user accounts that are under the control of Exchange Resource Forest Management; the **Mailboxes** OU is intended to hold new shadow user accounts. Once a user account in the **Accounts** OU is mailbox-enabled, a shadow account along with a linked mailbox is created in the **Mailboxes** OU and associated with the user account from the **Accounts** OU, to provide access to the mailbox.

Under these assumptions, the following examples are considered:

- Creating a user account in the **Accounts** OU, with the option to create a mailbox for that user
- Creating a mailbox for an existing account from the **Accounts** OU

- Making changes to a mailbox-enabled user account in the **Accounts** OU, with the changes automatically applied to the shadow account in the **Mailboxes** OU
- Deprovisioning a mailbox-enabled user account in the **Accounts** OU, with the shadow account automatically deprovisioned in the **Mailboxes** OU

Mailbox creation

This section demonstrates how Exchange Resource Forest Management automates creation of mailboxes in the Exchange forest for user accounts held in an accounts forest. The following examples are considered:

- Creating a new user account with a mailbox
- Creating a mailbox for an existing user account

Creating a new user account with a mailbox

You can use the Active Roles Web Interface to create a new user account in the accounts forest while having Exchange Resource Forest Management create a linked mailbox for that user account in the Exchange forest.

To create a new user account with a mailbox

1. In the Web Interface, select the **Accounts** OU, and then choose the **New User** command.
2. Fill in the fields on the pages for creating a user account.
3. Select the **Create an Exchange mailbox** check box, modify the alias if necessary, and click **Browse** to select the appropriate mailbox database.

    The list in the **Select Mailbox Database** dialog box contains the mailbox databases found in the Exchange forest. The list can be restricted by applying an Exchange Mailbox AutoProvisioning policy to the **Mailboxes** OU in the Exchange forest.

4. Complete the pages for creating the user account.

As a result, a new shadow account with a linked mailbox is created in the **Mailboxes** OU. The user account you have created in the **Accounts** OU is specified as the linked master account for that mailbox.

Creating a mailbox for an existing user account

For the purpose of this section, assume that the **Accounts** OU contains a user account that does not have an Exchange mailbox. You can create such an account by leaving the **Create an Exchange mailbox** check box cleared on the pages for creating user accounts in the Active Roles Web Interface. Then, you can create a mailbox for that user account by using the Web Interface as follows.

To create a mailbox for an existing user account

1. In the Web Interface, select the user account in the **Accounts** OU, and then choose the **Create User Mailbox** command.

2. On the **Mailbox Settings** page, modify the alias if necessary, and click **Browse** to select the appropriate mailbox database.

   The list in the **Select Mailbox Database** dialog box contains the mailbox databases found in the Exchange forest. The list can be restricted by applying an Exchange Mailbox AutoProvisioning policy to the **Mailboxes** OU in the Exchange forest.

3. Click **Finish**.

As a result, a new shadow account with a linked mailbox is created in the **Mailboxes** OU. The user account you selected in the **Accounts** OU is specified as the linked master account for that mailbox.

Account modification

This section demonstrates how Exchange Resource Forest Management handles the changes you make to a master account. Making changes to certain properties results in updating data in both the master account and shadow account, whereas modification of some other properties only updates data in the shadow account. Therefore, two examples are considered:

- Making changes to synchronized properties
- Making changes to substituted properties

Making changes to synchronized properties

When you update certain properties of a master account, Exchange Resource Forest Management updates those properties in both the master account and shadow account. These properties are referred to as *synchronized properties*. For details, see Synchronized properties earlier in this document.

To verify the behavior of synchronized properties

1. In the Web Interface, select a mailbox-enabled user account held in the **Accounts** OU, and then choose the **General Properties** command.

2. On the **General** tab, make changes to the **First name** or **Last name** field.

3. Go to the **Organization** tab and make changes to the **Title**, **Department**, or **Company** field.

4. Click **Save** to apply your changes.

5. Locate the shadow account in the **Mailboxes** OU—the name of the shadow account is identical to the name of the master account you have modified in the **Accounts** OU.

6. Choose the **Properties** command for the shadow account.

7. Examine data on the **General** and **Organization** tabs to verify that the changes you have made to the master account are also applied to the shadow account.

You can review the updates to the account properties by using the **Change History** command on the master account and on the shadow account—the Change History results provide information on which properties were updated, what changes were made to the properties, who performed the update, and when.

Making changes to substituted properties

When you view or change certain properties of a master account in an accounts forest, Exchange Resource Forest Management redirects the retrieval or change request to the properties of the shadow account in the Exchange forest. Such properties are referred to as *substituted properties*.

All the substituted properties that are mandatory for Exchange Resource Forest Management to work are listed in the Substituted properties section, earlier in this document. These properties used to store mailbox settings. As mailboxes are located in the Exchange forest, the updates to such properties need to be performed on the shadow accounts. Exchange Resource Forest Management implements a mechanism for capturing updates to substituted properties on the master account side and then applying those changes on the shadow account side.

You can view or modify some of the substituted properties on the Web Interface pages for managing Exchange recipient properties of a mailbox-enabled user account in the **Accounts** OU.

To view or change Exchange properties on the master account

1. In the Web Interface, select a mailbox-enabled user account held in the **Accounts** OU, and then choose the **Exchange Properties** command.

2. View or change the settings on the following tabs:

   - **General**
   - **E-mail Addresses**

- **Mailbox Features**
- **Mail Flow Settings**
- **Mailbox Settings**

3. Click **Save** to apply your changes.

Once you have completed these steps, your changes are applied to the shadow account associated with the master account you were administering. You can verify this by using the **Change History** command on the shadow account. The Change History results indicate that the changes were actually made to the properties of the shadow account, in the **Mailboxes** OU.

Account deprovisioning

When you use Active Roles to deprovision a master account, Exchange Resource Forest Management causes Active Roles to deprovision the shadow accounts as well. In this way, Active Roles deprovisions the master account's mailbox. You can verify this behavior by using the Active Roles Web Interface.

To deprovision a master account

- In the Web Interface, select a mailbox-enabled user account held in the **Accounts** OU, and then choose the **Deprovision** command.

Once you have completed these steps, the **Deprovision** command is performed not only on the master account but also on the shadow account. You can verify this by using the **Deprovisioning Results** command on the shadow account in the **Mailboxes** OU.

Membership management delegation

This section shows how Exchange Resource Forest Management facilitates delegation of the membership management task for distribution lists. To perform the procedures in this section, you need the following environment:

- Exchange Resource Forest Management configured as described in the Configuration section earlier in this document.
- A mailbox-enabled user account named **John Smith** created by Active Roles in the **Accounts** OU, so the shadow account for that user account exists in the **Mailboxes** OU.
- For the user account **John Smith**, on a computer in the accounts forest, Microsoft Outlook configured to connect to the mailbox of that user account.
- A mail-enabled group named **DL**, representing a certain distribution list, created in the **Mailboxes** OU.

The following procedure demonstrates how to delegate the task of managing the **DL** membership list to the user account **John Smith**.

To delegate the membership management task

1. In the Active Roles Web Interface for Administrators, open the **Exchange Properties** page for the user account **John Smith**:

    - Locate and select the **Accounts** OU.
    - Select the user account **John Smith** in the list of objects held in that OU.
    - Click the **Exchange Properties** command.

2. On the **Exchange Properties** page, go to the **Shadow Account** tab, and click the **Properties** button on that tab.

    This opens the **General Properties** page for the shadow account.

3. On the **General Properties** page, click the **Account** tab and note down the pre-Windows 2000 logon name of the shadow account.

4. In the Web Interface, open the **Managed by** tab for the **DL** group:

    - Locate and select the **Mailboxes** OU.
    - Click the **DL** group in the list of objects held in that OU.
    - Click the **Managed by** tab on the **General Properties** page that appears.

5. On the **Managed by** tab, click the **Change** button under the **Manager** box.

    This opens the **Select Object** dialog box allowing you to specify the manager account.

6. Use the **Select Object** dialog box to find and select the shadow account:

    - In the **Name** box, type the name of the shadow account you noted down in Step 3.
    - Click **Search**.
    - Click **Search**.
    - In the list of search results, click the name of the shadow account.
    - Click **OK** to close the **Select Object** dialog box.

7. On the **Managed by** tab, click **Save**; then, select the **Manager can update membership list** check box, and click **Save** again.

Although you have specified the shadow account as the manager of the group, Active Roles updates security settings on the group so that the master account is authorized to add or remove members from the group by using conventional tools such as Microsoft Outlook.

If you clear the **Manager can update membership list** check box, or change the manager of the group, Active Roles updates the security settings to revoke the former manager's right to modify the membership list of the group.

After you have specified the shadow account as the manager of the **DL** group with the **Manager can update membership list** option, force Active Roles to give the manager rights to the master account by executing the scheduled task **ERFM - Mailbox Management** held in the **Configuration/Server Configuration/Scheduled**

Tasks/Builtin container or wait for a scheduled run of that task. Then, you can verify that the master account can use Microsoft Outlook to add or remove group members, provided that Outlook is configured to connect to the mailbox for the **John Smith** user account:

1. Log on with the name and password of the **John Smith** account to the computer where Microsoft Outlook is configured to connect to the linked mailbox of that user account.

2. Open Outlook and press Ctrl+Shift+B to display the Address Book.

3. In the Address Book, double-click the **DL** group.

4. On the **General** tab in the dialog box that appears, click **Modify Members** to add or remove members from the **DL** group.

Mailbox type conversion

This section demonstrates how to perform mailbox type conversion using Active Roles . The following scenarios are covered:

- Converting a linked mailbox to a user mailbox
- Converting a user mailbox to a linked mailbox

Converting a linked mailbox to a user mailbox

If a given mailbox from the Exchange forest is assigned to a user from an accounts forest (linked mailbox), then you can use Active Roles to convert that mailbox to the user mailbox type. After you convert the mailbox, the external user (formerly master account) can no longer access the mailbox. The mailbox can only be accessed by the user account that is associated with the mailbox in the Exchange forest (formerly shadow account).

To convert a linked mailbox to a user mailbox

1. Open the Active Roles Web Interface for Administrators, and select the mailbox user account in the Exchange forest (shadow account).

2. Click the **Convert to User Mailbox** command.

3. Click **OK** in the confirmation message box that appears.

After mailbox conversion, the mailbox user account remains disabled. To enable the user account, set the user password by using the **Reset Password** command, and then click the **Enable Account** command.

Converting a user mailbox to a linked mailbox

For a user mailbox in the Exchange forest, you can use Active Roles to assign that mailbox to a user from an accounts forest. This configures the mailbox as follows:

- The mailbox type changes to the linked mailbox type.
- The user from the accounts forest becomes the master account for the mailbox.
- The user associated with the mailbox in the Exchange forest becomes the shadow account.

The domain of the user from the accounts forest must be registered with Active Roles (managed domain).

To convert a user mailbox to a linked mailbox

1. Open the Active Roles Web Interface for Administrators, and select the user mailbox in the Exchange forest.
2. Click the **Convert to Linked Mailbox** command.
3. Click **Change** under the **Linked master account** field, and select the user from an accounts forest.
4. Click **Finish**.

As a result of these steps, the master account is assigned to the mailbox and the mailbox user in the Exchange forest becomes the shadow account, linked with the master account. If the master account is in the scope of the Exchange Resource Forest Management policy, the properties of the master account and shadow account are synchronized in the same way as when you configure a mailbox-enabled user in an accounts forest by using the Exchange Resource Forest Management solution.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product